适用于物联网通信的无证书聚合签密算法 *

胡荣磊，李文敬，蒋 华，曾 萍，王庆瑞，陈 雷

(北京电子科技学院 通信工程系，北京 100070)

摘 要：针对目前无证书聚合签密（CLASC）方案计算效率较低的问题，提出了一个适合于物联网的无双线性对的聚合签密方案。该方案与目前最好方案[15]相比，运算效率提高了近六倍，在聚合签密阶段只需要（2n+1）次点乘运算，在聚合解签密阶段需要（5n+1）次点乘运算。基于离散对数问题，在随机预言模型下证明了方案满足机密性和不可伪造性。在聚合签密验证阶段，不需要第三方的秘密信息，方案满足可公开验证性。最后，指出该方案能以较低的计算速率实现较高的安全性，更适合用于物联网。

关键词：无证书聚合签密；物联网；无双线性对；随机预言模型；可公开验证

中图分类号：TP309.7 doi: 10.19734/j.issn.1001-3695.2018.05.0446

Certificateless aggregate signcryption scheme for internet of things communication

Hu Ronglei, Li Wenjing, Jiang Hua, Zeng Ping, Wang Qingrui, Chen Lei

(*Dept. of Communication Engineering*, *Beijing Electronic Science & Technology Institute*, *Beijing* 100070, *China*)

Abstract: Aiming at the problem of low computational efficiency of the current certificateless aggregation signcryption (CLASC) scheme, this paper proposed an aggregate signcryption scheme which is suitable for the Internet of things without bilinear pairings. Compared with the current best scheme[15], the efficiency of the scheme is increased by nearly 6 times. The scheme only needs (2n+1) times of dot multiplication operation in the aggregate signcryption stage, and (5n+1) times of dot multiplication operation in the aggregate unsigncryption stage. Based on the discrete logarithm problem, the scheme satisfied confidentiality and the unforgeability under the random oracle model. In the aggregate signcryption verification phase, there is no need to provide the third party's secret information, so the scheme satisfies public verifiability. Finally, it also pointed out that the scheme can achieve higher security at lower computation speed and is more suitable for Internet of things.

Key words: certificateless aggregate signcryption; Internet of things; without bilinear pairings; random oracle model; publicly verifiability

0 引言

2005 年，国际电信联盟首次提出物联网（Internet of things，IoT）的概念[1]。之后，越来越多的国家投入了对物联网的研究，并取得了丰硕的成果[2~5]。物联网已经广泛运用于食品安全、公共安全、健康监测、智能交通、安防、环保等诸多行业。网络规模从一个实验室到一栋大楼再到一个小区不断扩大，并且出现了不同系统的融合。随着网络规模的扩大，也暴露出物联网系统的问题：物联网终端分布广，而且结构较计算机网络的终端更为简单，面临终端功能欠缺和容易遭受攻击的缺点。而物联网的应用行业如食品安全、入侵检测等则要求物联网能够对突发事件、使用者和管理者提供快速、准确的响应，实现人与物的准确交流，同时还需要保证网络基础设施有一个经济的部署。这就需要系统在一个高效、可靠、安全的模式下协调运行，所以利用密码技术设计安全、高效的算法与协议是 IoT 研究的侧重点。

保证信息安全的核心技术就是现代密码技术，它可以保证网络环境下信息的保密性、完整性、可用性和抗抵赖性等。其中，保密性可以通过加密的方法来实现，认证性可以用数字签名来实现。如果需要同时实现保密性和认证性，传统的公钥密码技术是使用“先签名再加密”的方式，但这种方法效率低下。1997 年，Zheng 等人[6]提出了签密的概念并给出了具体的方案。2002 年，Baek 等人[7]首次定义了签密方案的安全模型。

在实际应用中，当签密用户较多时，接受者需要同时验证

收稿日期：2018-05-14；**修回日期**：2018-07-10 **基金项目**：中央高校基本科研业务费资助项目（2017LG-01）

作者简介：胡荣磊（1977-），男，河北衡水人，副研究员，博士，主要研究方向为通信与信息系统、信息安全；李文敬（1992-），女，山东济宁人，硕士研究生，主要研究方向为信息安全（2654019946@qq.com）；蒋华（1962-），山西大同人，教授，博士，主要研究方向为通信与信息安全；曾萍（1969-），女，广东潮安人，教授，博士，主要研究方向为无线网络安全；王庆瑞（1993-），男，山东聊城人，硕士研究生，主要研究方向为信息安全；陈雷（1992-），男，河北邯郸人，硕士研究生，主要研究方向为信息安全.

多个密文。为了提高密文的批验证效率，2009 年，Selvi 等人[8]结合聚合签名[9]的优势提出了聚合签密的概念。2003 年，Al-Riyami 等人[10]首次提出了无证书密码（certificateless aggregate signcryption，CLASC）体制，该密码体制不仅避免了公钥证书管理及验证问题，而且很好地解决了密钥托管问题。2008 年，Barbosa 等人[11]首次提出了一个无证书签密方案并给出了其对应的安全模型。随后，Eslami 等人[12]、刘建华等人[13]、牛淑芬等人[14] 和 Han 等[15]又各自提出无证书签密方案。

通过对聚合密码体制的研究，本文提出了一种适合物联网系统的不需要双线性运算的无证书签密方案。因为没有复杂的双线性对运算，该方案具有较高的运算效率。经证明，该方案满足不可伪造性、机密性和可公开验证性。

1　预备知识

定义在 F_p（F_p 表示有 p 个元素的有限域，p 为素数且>3）上椭圆曲线方程为

$$y^2 = x^3 + ax + b \quad a,b \in F_p$$

判别式为

$$4a^3 + 27b^2 \neq 0 \bmod p$$

椭圆曲线上的所有解与一个无穷远点 O 构成的一个集合用 $E(F_P)$ 来表示，即：$E(F_P) = \{(x,y) \mid x,y \in F_p$ ｝，且满足方程｛$y^2 = x^3 + ax + b$ ｝$\cup \{O\}$，$E(F_P)$ 上点的数目用 q 表示，成为椭圆曲线的阶。

1.1　离散对数问题

离散对数问题（Discrete logarithm problem，DLP）：设 G 是一个阶为 q 的加法循环群，P 是 G 的生成元，对于 $b \in Z_q^*$，找到整数 a 使得 $b = aP$ 是困难的。

1.2　计算 Diffie-Hellman 问题

计算 Diffie-Hellman 问题（Computational Diffie-Hellman Problem，CDHP）：对于未知的 $a,b \in Z_q^*$，给定（aP,bP），计算 abP 是困难的。

2　适合于物联网的不含双线性对的无证书聚合签密方案

本文提出了一个适用于物联网[16]的的无证书聚合签密方案。一个完整的物联网由感知节点（sensory node，SN_i，$1 \le i \le n$）、网关节点（gateway node，GN）、云平台服务器（cloud platform server，CPS）和应用终端（application terminal，AT）组成,，如图 1 所示。

感知节点的功能是将收集到的数据沿着其他感知节点进行逐跳地传输，并发送到网关节点。网关节点将数据自动保存，并在一定的时间间隔内将自动收集的数据周期性的传输至互联网云平台服务器。云平台服务器将得到的数据发送给应用终端，以供应用终端解密、分析。其中云平台服务器是诚实可靠地，负责系统管理与维护，包括对 SN、GN 和 AT 的登记，私钥分发等。云平台服务器与 GN，GN 与 SN，GN 与 GN 之间是通过无线通信。具体实现过程如下：

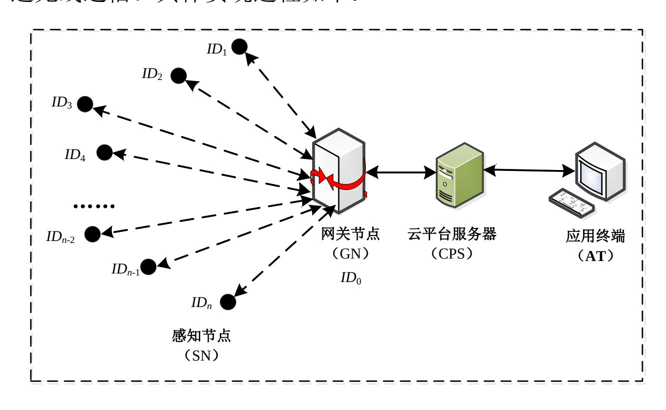


图 1　无线传感器网络的物联网结构

Fig.1 IoT architecture of WSN

a）系统初始化，该算法由 GN 执行。输入安全参数 k，选择一个大素数 q（$q > 2^k$），设 G 为椭圆曲线的一个循环群，P 为 G 的生成元。选择三个抗碰撞的杂凑函数 $H_1:\{0,1\}^* \times G \times G \to Z_q^*$，$H_2: G \times G \to Z_q^*$，$H_3, H_4$：$G \times G \times G \times G \to Z_q^*$。CPS 随机选择主密钥 $s \in Z_q^*$，并将其秘密保存，计算主公钥：$P_{pub} = sP$，CPS 发布系统公开参数 params=$\{q, P, G, P_{pub}, H_1, H_2, H_3\}$　。

b）密钥生成，该算法由感知节点 SN_i 执行。感知节点 SN_i 随机选取秘密值 $x_i \in Z_q^*$，并将其保存，计算 $X_i = x_i P$，将（ID_i，X_i）发送给 CPS。其中，x_i 为私钥，X_i 为公钥。

c)部分私钥生成，该算法由 CPS 执行。CPS 随机选择秘密值 $r_i \in Z_q^*$，计算 $R_i = r_i P$，$h_{i1} = H_1(ID_i, R_i, X_i)$，$D_i = r_i + sh_{i1}$，并将（$R_i$，$D_i$）通过安全信道发送给各感知节点 SN_i。其中，R_i 作为用户部分公钥，D_i 作为用户的部分私钥。

这样，SN_i 的私钥为 $SK_i = (D_i, x_i)$，公钥为 $PK_i = (R_i, X_i)$。同样，应用终端 AT 的私钥为 $SK_B = (D_B, x_B)$，公钥为 $PK_B = (R_B, X_B)$。

d)个体签密，该算法由感知节点 SN_i 执行。感知节点 SN_i 发送给 AT 的消息 m_i 进行签密的步骤如下：

①感知节点 SN_i 随机选取 $k_i, t_i \in Z_q^*$。

②计算 $K_i = k_i P$，$T_i = t_i P$；

③计算 $Q_{i1} = k_i X_B$，$Q_{i2} = t_i(R_B + P_{pub} H_1(ID_B, R_B, X_B))$；

④计算 $h_{i2} = H_2(Q_{i1}, Q_{i2})$；

⑤加密，$C_i = h_{i2} \oplus (m_i \| ID_i)$；

⑥计算 $h_{i3} = H_3(C_i, Q_{i1}, Q_{i2}, K_i)$，$h_{i4} = H_4(C_i, Q_{i1}, Q_{i2}, T_i)$；

⑦签名，$S_i = k_i + t_i + h_{i3} D_i + h_{i4} x_i$。

感知节点 SN_i 发送给 AT 的关于 m_i 的签密为：$\sigma_i = (C_i, K_i, T_i, S_i)$（$1 \le i \le n$）。

e)聚合签密，该算法由网关节点 CN 执行。

收到 n 个签密者信息 $\sigma_i = (C_i, K_i, T_i, S_i)$（$1 \le i \le n$），聚合者 CN 计算 $S = \sum_{i=1}^{n} S_i$，则聚合签密为 $\sigma = \langle \{K_i, T_i, C_i\}_{i=1}^{n}, S \rangle$，并将其发送给 AT。

f)解签密，该算法由应用终端 AT 执行。

应用终端 AT 对 SN_i 发送的签密 $\sigma_i = (C_i, K_i, T_i, S_i)$ 解密步骤

为：

①计算 $Q_{i1}=K_i x_B$，

$Q_{i2}=T_i(r_B+sH_1(ID_B,R_B,X_B))=T_iD_B$；

②计算 $h_{i2}=H_2(Q_{i1},Q_{i2})$；

②恢复明文，$(m_i \| ID_i)=C_i\oplus h_{i2}$；

④计算 $h_{i3}=H_3(C_i,Q_{i1},Q_{i2},K_i)$，

$h_{i4}=H_4(C_i,Q_{i1},Q_{i2},T_i)$；

验证签名的正确性:

$S_iP=K_i+T_i+h_{i3}(R_i+P_{pub}H_1(ID_i,R_i,X_i))+h_{i4}X_i$

如果成立，证明聚合签密是有效的，输出 $m_i \| ID_i$，否则，输出为“false”。

g)聚合解签密，该算法由应用终端 AT 执行。

AT 对 SN_i 发送的签密 $\sigma=<\{K_i,T_i,C_i\}_{i=1}^{n},S>$ 解密步骤为:

①计算 $Q_{i1}=K_i x_B$，

$Q_{i2}=T_i(r_B+sH_1(ID_B,R_B,X_B))=T_iD_B$；

②计算 $h_{i2}=H_2(Q_{i1},Q_{i2})$；

③恢复明文，$(m_i \| ID_i)=h_{i2}\oplus C_i$

④计算 $h_{i3}=H_3(C_i,Q_{i1},Q_{i2},K_i)$，

$h_{i4}=H_4(C_i,Q_{i1},Q_{i2},T_i)$；

验证签名的正确性:

$$SP=\sum_{i=1}^{n}K_i+\sum_{i=1}^{n}T_i+\sum_{i=1}^{n}[h_{i3}(R_i+P_{pub}H_1(ID_i,R_i,X_i))]+\sum_{i=1}^{n}h_{i4}X_i$$

如果成立，证明聚合签密是有效的，输出 $m_i \| ID_i$，否则，输出为“false”

3　方案分析

3.1　正确性

定理 1　接收者能够验证签密、聚合签密的正确性，并能得到正确的解密明文 m_i。

证明　a）AT 能够验证签密 $\sigma_i=(C_i,K_i,T_i,S_i)$（$1\le i\le n$）的正确性。

$$\begin{aligned}S_iP&=[k_i+t_i+h_{i3}D_i+h_{i4}x_i]P\\&=[k_i+t_i+h_{i3}(r_i+sh_{i1})+h_{i4}x_i]P\\&=K_i+T_i+h_{i3}(R_i+P_{pub}H_1(ID_i,R_i,X_i))+h_{i4}X_i\end{aligned}$$

b)AT 能够验证聚合签密 $\sigma=<\{K_i,T_i,C_i\}_{i=1}^{n},S>$ 的正确性。

$$\begin{aligned}SP&=\sum_{i=1}^{n}[k_i+t_i+h_{i3}D_i+h_{i4}x_i]P\\&=\sum_{i=1}^{n}[K_i+T_i+h_{i3}D_i+h_{i4}(R_i+P_{pub}H_1(ID_i,R_i,X_i))]\\&=\sum_{i=1}^{n}K_i+\sum_{i=1}^{n}T_i+\sum_{i=1}^{n}[h_{i3}(R_i+P_{pub}H_1(ID_i,R_i,X_i))]+\sum_{i=1}^{n}h_{i4}D_i\end{aligned}$$

c)AT 能够得到正确解密明文 m_i。

$$\begin{aligned}h_{i2}&=H_2(Q_{i1},Q_{i2})\\&=H_2(k_iX_B,t_i(X_B+R_B+P_{pub}H_1(ID_B,R_B,X_B)))\\&=H_2(k_ix_BP,t_iP(x_B+r_B+sH_1(ID_B,R_B,X_B)))\\&=H_2(K_ix_B,T_i(x_B+r_B+sH_1(ID_B,R_B,X_B)))\\&=H_2(K_ix_B,T_iD_B)=h_{i2}'\end{aligned}$$

由于 SN_i 通过计算 $C_i=h_{i2}\oplus(m_i \| ID_i)$ 对明文进行加密，AT 通过计算 $m_i \| ID_i=h_{i2}'\oplus C_i$ 对密文进行解密，又由于 $h_{i2}=h_{i2}'$，所以可以确保 CPS 最后得到正确的明文。

3.2　不可伪造性

定理 2　在随机预言模型中且 DLP 难解的情况下，本文提出 CLASC 方案在适应性选择消息攻击下是存在性不可伪造的（EUF-CLASC-CMA）。

引理 1　随机预言模型下，如果存在一个概率多项式时间攻击者 A_1 以不可忽略的概率赢得游戏，那么存在算法 $\check{C}_1$ 能够解决 DLP 问题（其中，A_1 最多执行 q_{H_i}（$i=1,2,3,4$）次 H_i 问询、q_{SK} 次私钥问询、q_{PSK} 次部分私钥问询、q_{PK} 次公钥问询以及 q_{SC} 次签密问询，聚合签名的用户数为 n）。

证明　假设算法 $\check{C}_1$ 是一个 DLP 的解决者，输入元组为（P，bP），其中 $b\in Z_q^*$ 且未知，目标是计算 b，以 A_1 作为子程序的挑战者。$\check{C}_1$ 维护以下 6 个列表 L_1、L_2、L_3、L_4、L_{ID}、L_{SC} 分别记录 A_1 对预言机 H_1、H_2、H_3、H_4、创建用户、签密的问询数据，列表初始化均为空。

1）系统初始化阶段。

$\check{C}_1$ 设 $P_{pub}=bP$（这里 b 默认作为系统主密钥，并且对 A_1 保密），选择并发送系统参数 params=$\{q,P,G,P_{pub},H_1,H_2,H_3\}$ 给敌手 A_1。

2）问询阶段

H_1 问询。$\check{C}_1$ 维护列表 $L_1=\{ID_i,R_i,X_i,h_{i1}\}$。当 A_1 输入 (ID_i,R_i,X_i)，$\check{C}_1$ 作出以下回应:

a)若该 (ID_i,R_i,X_i) 对应的问询已存在于列表 L_1 中，则返回对应的 h_{i1} 给 A_1。

b)否则，$\check{C}_1$ 随机选择 $h_{i1}\in Z_q^*$，将（ID_i,R_i,X_i,h_{i1}）加入列表 L_1 中，并返回 h_{i1} 给 A_1。

H_2 问询。$\check{C}_1$ 维护列表 $L_2=\{Q_{i1},Q_{i2},h_{i2}\}$。当 A_1 输入 (Q_{i1},Q_{i2})，$\check{C}_1$ 作出以下回应:

a)若该 (Q_{i1},Q_{i2}) 对应的问询已存在于列表 L_2 中，则返回对应的 h_{i2} 给 A_1。

b)否则，$\check{C}_1$ 随机选择 $h_{i2}\in Z_q^*$，将（Q_{i1},Q_{i2},h_{i2}）加入列表 L_2 中，并返回 h_{i2} 给 A_1。

H_3 问询。$\check{C}_1$ 维护列表 $L_3=\{C_i,Q_{i1},Q_{i2},K_i,h_{i3}\}$。当 A_1 输入 (C_i,Q_{i1},Q_{i2},K_i)，$\check{C}_1$ 作出以下回应:

a)若该 (C_i,Q_{i1},Q_{i2},K_i) 对应的问询已存在于列表 L_3 中，则返回对应的 h_{i3} 给 A_1。

b)否则，$\check{C}_1$ 随机选择 $h_{i3}\in Z_q^*$，将（$C_i,Q_{i1},Q_{i2},K_i,h_{i3}$）加入列表 L_3 中，并返回 h_{i3} 给 A_1。

H_4 问询。$\check{C}_1$ 维护列表 $L_4=\{C_i,Q_{i1},Q_{i2},T_i,h_{i4}\}$。当 A_1 输入 (C_i,Q_{i1},Q_{i2},T_i)，$\check{C}_1$ 作出以下回应:

a)若该 (C_i,Q_{i1},Q_{i2},T_i) 对应的问询已存在于列表 L_4 中，则返回对应的 h_{i4} 给 A_1。

b)否则，$\check{C}_1$ 随机选择 $h_{i4}\in Z_q^*$，将（$C_i,Q_{i1},Q_{i2},T_i,h_{i4}$）加入列表 L_4 中，并返回 h_{i4} 给 A_1。

用户创建问询。$\check{C}_1$ 维护初始为空的列表 $L_{ID_i}=\{ID_i,h_{i1},D_i,r_i,R_i,x_i,X_i\}$。提交用户身份 ID_i，如果（$ID_i,h_{i1},D_i,r_i,R_i,x_i,X_i$）在 L_{ID_i} 中已存在，则忽略；否则，$\check{C}_1$ 执行 H_1 询问，取得 h_{i1}，然后：

a)如果 $ID_i=ID_j$，$\check{C}_1$ 随机选择 r_j，$x_j\in Z_q^*$，计算 $R_j=r_jP$ 和 $X_j=x_jP$，将（$ID_j,h_{j1},\perp,r_j,R_j,x_j,X_j$）插入 L_{ID}；

b)否则，$\check{C}_1$ 随机选择 $D_i,x_i\in Z_q^*$，计算 $R_i=D_iP-h_{i1}P_{pub}$ 和 $X_i=x_iP$，将（$ID_i,h_{i1},D_i,\perp,R_i,x_i,X_i$）插入 L_{ID}。

部分私钥问询。$A_{\rm I}$ 提交用户身份 ID_i，$\check{C}_1$ 作出以下回应：

a)如果 $ID_i=ID_j$，$\check{C}$ 终止游戏；

b)否则，$\check{C}_1$ 返回 D_i 给 $A_{\rm I}$。

私钥问询。$A_{\rm I}$ 提交用户身份 ID_i，$\check{C}_1$ 则返回对应的 x_i 给 $A_{\rm I}$。

公钥问询。$A_{\rm I}$ 提交用户 ID_i，$\check{C}_1$ 返回 ID_i 对应的公钥（R_i,X_i）作为应答。

公钥替换问询。$A_{\rm I}$ 用一个新的公钥（X_i',R_i'），替换合法签密者 ID_i 的原公钥（X_i,R_i）。

签密问询。$\check{C}_1$ 维护初始为空的列表 $L_{SC}=\{m_i,ID_i,ID_B,K_i,T_i,h_{i2},h_{i3},h_{i4},S_i,c_i\}$。$A_{\rm I}$ 提交待签密消息 m_i、发送者身份 ID_i 和接受者身份 ID_B。

a)如果 $ID_i=ID_j$，$\check{C}_1$ 随机选择 $S_i,h_{i3},h_{i4},k_i\in Z_q^*$，计算 $K_i=k_iP$，$T_i=S_iP-h_{i3}x_j-h_{i4}D_j-K_i$ 和 $h_{i2}=H_2(K_ix_B,T_i(x_B+r_B+sH_1(ID_B,R_B,X_B)))$，查询列表 L_3 和 L_4，如果 L_3 中存在（$C_i,Q_{i1},Q_{i2},K_i,h_{i3}'$）或 L_4 中存在（$C_i,Q_{i1},Q_{i2},T_i,h_{i4}'$），且 $h_{i3}\neq h_{i3}'\vee h_{i4}\neq h_{i4}'$，$\check{C}_1$ 重新选择 S_i,h_{i3},h_{i4},k_i；否则，$\check{C}_1$ 计算 $C_i=h_{i2}\oplus(m_i\,\|\,ID_i)$，返回密文 $\sigma_i=(C_i,K_i,T_i,S_i)$；

b)否则 $ID_i\neq ID_j$，$\check{C}_1$ 按照签密算法进行计算，并根据需要执行 H_i（$i=1,2,3,4$）问询和密钥问询，然后返回签密密文 $\sigma_i=(C_i,K_i,T_i,S_i)$；

最后，$\check{C}_1$ 将（$m_i,ID_i,ID_B,K_i,T_i,h_{i2},h_{i3},h_{i4},S_i,c_i$）插入到 L_{SC} 中，将（$C_i,Q_{i1},Q_{i2},K_i,h_{i3}$）和（$C_i,Q_{i1},Q_{i2},T_i,h_{i4}$）分别插入到 L_3 和 L_4。

3）伪造阶段

询问阶段结束后，$A_{\rm I}$ 提交挑战用户身份（ID_j,ID_B）、挑战消息 m_j 及其签密密文 (C_j,K_j,T_j,S_j)。

$\check{C}_1$ 计算 $h_{i2}=H_2(K_ix_B,T_i(x_B+r_B+sH_1(ID_B,R_B,,X_B)))$，解密消息 $m_j=h_{i2}\oplus C_j$。根据分叉引理[17]，$\check{C}_1$ 利用预言机重放攻击技术可以得到两个合法的签名 $\{m_j,ID_j,ID_B,K_j,T_j,h_{j3},h_{j4},S_j\}$ 和 $\{m_j,ID_j,ID_B,K_j,T_j,h_{j3}',h_{j4},S_j'\}$。其中 $S_i\neq S_i'$，$h_{j3}\neq h_{j3}'$，并且满足：

$$S_j=k_j+t_j+h_{j3}D_j+h_{j4}x_i$$

$$S_j'=k_j+t_j+h_{j3}'D_j+h_{j4}x_i$$

那么，$\check{C}_1$ 计算：

$$S_j'-S_j=k_j+t_j+h_{j3}'D_j+h_{j4}x_i-\left(k_j+t_j+h_{j3}D_j+h_{j4}x_i\right)$$

$$=(h_{j3}'-h_{j3})D_j$$

$$b=\frac{(D_j-r_j)}{H_1(ID_j,R_j,X_j)}=\frac{S_j'-S_j-(h_{j3}'-h_{j3})r_j}{(h_{j3}'-h_{j3})H_1(ID_j,R_j,X_j)}$$，作为对 DLP 的回答。

因此，$\check{C}_1$ 成功获得 DLP 困难问题的一个实例。$\check{C}_1$ 能够成功解决 DLP 困难问题的优势为 $\varepsilon'=\frac{1}{q_{PSK}+n}\left(1-\frac{1}{q_{PSK}+n}\right)^{q_{PSK}+n-1}\varepsilon$。证毕。

引理 2 随机预言模型下，如果存在一个概率多项式时间攻击者 $A_{\rm II}$ 以不可忽略的概率赢得游戏，那么存在算法 $\check{C}_2$ 能够解决 DLP 问题（其中，$A_{\rm II}$ 最多执行 q_{H_i}（$i=1,2,3,4$）次 H_i 问询、q_{SK} 次私钥问询、q_{PSK} 次部分私钥问询、q_{PK} 次公钥问询以及 q_{SC} 次签密问询，聚合签名的用户数为 n）。

证明：假设算法 $\check{C}_2$ 是一个 DLP 的解决者，输入元组为（P，bP），其中 $b\in Z_q^*$ 且未知，目标是计算 b，以 $A_{\rm I}$ 作为子程序的挑战者。$\check{C}_1$ 维护以下 6 个列表 L_1、L_2、L_3、L_4、L_{ID}、L_{SC} 分别记录 $A_{\rm I}$ 对预言机 H_1、H_2、H_3、H_4、创建用户、签密的问询数据，列表初始化均为空。

1）系统初始化阶段

设 $P_{pub}=sP$，$s\in Z_q^*$，生成系统参数 params=$\{q,P,G,P_{pub},H_1,H_2,H_3\}$。$\check{C}_2$ 发送（q,P,G,P_{pub},s）给 $A_{\rm II}$。

2）问询阶段

$A_{\rm II}$ 执行多项式有界次的以下问询。

H_1、H_2、H_3 和 H_4 问询，与定理 1 相同。

用户创建问询。$\check{C}_2$ 维护初始为空的列表 $L_{ID_i}=\{ID_i,h_{i1},D_i,r_i,R_i,x_i,X_i\}$。提交用户身份 ID_i，如果 $\{ID_i,h_{i1},D_i,r_i,R_i,x_i,X_i\}$ 在 L_{ID_i} 中已存在，则忽略；否则，$\check{C}_2$ 执行 H_1 询问，取得 h_{i1}，然后：

a) 如果 $ID_i=ID_j$，令 $X_j=bP$，计算 $R_j=r_jP$ 和 $D_j=r_j+sH_1(ID_j,R_j,X_j)$，将（$ID_j,h_{j1},\perp,r_j,R_j,x_j,X_j$）插入 L_{ID}；

b)否则，$\check{C}_2$ 随机选择 D_i，$x_i\in Z_q^*$，计算 $R_i=r_iP$、$D_i=r_i+sh_{i1}$ 和 $X_i=x_iP$，将（$ID_i,h_{i1},D_i,\perp,R_i,x_i,X_i$）插入 L_{ID_i}。

部分私钥问询。$A_{\rm II}$ 提交用户身份 ID_i，$\check{C}_2$ 则返回对应的 D_i 给 $A_{\rm II}$。

私钥问询。$A_{\rm II}$ 提交用户身份 ID_i，$\check{C}_2$ 作出以下回应：

a)如果 $ID_i=ID_j$，$\check{C}_2$ 终止游戏；

b)否则，$\check{C}_2$ 返回 x_i 给 $A_{\rm I}$。

公钥问询。$A_{\rm II}$ 提交用户 ID_i，$\check{C}_2$ 返回 ID_i 对应的公钥（R_i,X_i）作为应答。

公钥替换问询。$A_{\rm II}$ 提交用户身份 ID_i，以及替换公钥 X_i'，如果 $ID_i=ID_j$，$\check{C}_2$ 终止游戏；否则 $\check{C}_2$ 用 X_i' 替换替换 ID_i 原有的公钥 X_i

签密问询。$\check{C}_2$ 维护初始的为空的列表 $L_{SC}=\{m_i,ID_i,ID_B,K_i,T_i,h_{i2},h_{i3},S_i,c_i\}$。$A_{\rm II}$ 提交待签密消息 m_i、发送者身份 ID_i 和接受者身份 ID_B。

a)如果 $ID_i=ID_j$，$\check{C}$ 随机选择 $S_i,h_{i3},t_i\in Z_q^*$，计算 $T_i=t_iP$，$K_i=S_iP-h_{i3}(x_j+D_j)-T_i$ 和 $h_{i2}=H_2(K_ix_B,T_i(x_B+r_B+sH_1(ID_B,R_B,X_B)))$，查询列表 L_3 和 L_4，如果 L_3 中存在（$C_i,Q_{i1},Q_{i2},K_i,h_{i3}'$）或 L_4 中存在（$C_i,Q_{i1},Q_{i2},T_i,h_{i4}'$），且 $h_{i3}\neq h_{i3}'\vee h_{i4}\neq h_{i4}'$，$\check{C}_2$ 重新选择 S_i,h_{i3},h_{i4},t_i；否则，$\check{C}_2$ 计算 $C_i=h_{i2}\oplus(m_i\,\|\,ID_i)$，返回密文 $\sigma_i=(C_i,K_i,T_i,S_i)$；

b)否则 $ID_i \neq ID_j$，$\check{C}_1$ 按照签密算法进行计算，并根据需要执行 H_i（$i=1,2,3,4$）问询和密钥问询，然后返回签密密文 $\sigma_i=(C_i,K_i,T_i,S_i)$；

最后，$\check{C}_2$ 将（$m_i,ID_i,ID_B,K_i,T_i,h_{i2},h_{i3},h_{i4},S_i,c_i$）插入到 L_{SC} 中，将（$C_i,Q_{i1},Q_{i2},K_i,h_{i3}$）和（$C_i,Q_{i1},Q_{i2},T_i,h_{i4}$）分别插入到 L_3 和 L_4。

3）伪造阶段

询问阶段结束后，A_{II} 提交挑战用户身份（ID_j,ID_B）、挑战消息 m_j 及其签密密文 (C_j,K_j,T_j,S_j)。

$\check{C}_2$ 计算 $h_{i2}=H_2(K_i x_B,T_i(x_B+r_B+sH_1(ID_B,R_B,\ X_B)))$，解密消息 $m_j=h_{i2}\oplus C_j$。根据分叉引理[17]，$\check{C}_2$ 利用预言机重放攻击技术可以得到两个合法的签名 $\{m_j,ID_j,ID_B,K_j,T_j,h_{j2},h_{j3},h_{j4},S_j\}$ 和 $\{m_j,ID_j,ID_B,K_j,\ T_j,h_{j2},h_{j3},h_{j4}',S_j'\}$。其中 $S_i\neq S_i'$，$h_{j3}\neq h_{j3}'$，并且满足：

$$S_j=k_j+t_j+h_{j3}D_j+h_{j4}x_i$$

$$S_j'=k_j+t_j+h_{j3}D_j+h_{j4}'x_i$$

那么 $\check{C}_2$ 计算：

$$S_j'-S_j=k_j+t_j+h_{j3}D_j+h_{j4}'x_j-\left(k_j+t_j+h_{j3}D_j+h_{j4}x_i\right)$$

$$=(h_{j4}'-h_{j4})x_j$$

$b=x_j=\dfrac{S_j'-S_j}{h_{j4}'-h_{j4}}$ 作为对 DLP 的回答。

因此，$\check{C}_2$ 成功获得 DLP 困难问题的一个实例。$\check{C}_2$ 能够成功解决 DLP 困难问题的优势为 $\varepsilon'=\dfrac{1}{q_{PSK}+n}\left(1-\dfrac{1}{q_{PSK}+n}\right)^{q_{PSK}+n-1}\varepsilon$。证毕。

3.3 机密性

定理 3 随机预言模型下，基于 CDHP，本文提出的 CLASC 方案在适应性选择密文攻击下是不可区分的，即 IND-CLASC-CCA2 安全。

引理 3 随机预言模型下，如果存在概率多项式时间敌手 A_I（或 A_{II}）以不可忽略的概率赢得游戏，则存在挑战者 $\check{C}$ 能够以不可忽略的概率解决 CDPH 的一个实例。

引理 3 的证明方法与文献[12]机密性证明方案类似，限于篇幅，略去此部分。

3.4 可公开验证性

本文方案中，当签密发送者和签名接受者关于聚合签密密文的真伪发生争执时，任意第三方均可验证下面等式：

$$SP=\sum_{i=1}^{n}K_i+\sum_{i=1}^{n}T_i+\sum_{i=1}^{n}[h_{i3}(R_i+P_{pub}H_1(ID_i,R_i,X_i))]+\sum_{i=1}^{n}h_{i4}X_i$$

因为该等式的验证无需接受者的参与，且不需要任何签密者的秘密信息，因此方案具有可公开验证性。

3.5 性能分析

为了便于比较签密方案的计算效率，假设参与签密的用户有 n 个，这里考虑三种运算：指数运算（标志为 e）、群 G 上的乘法运算（标志为 s）、双线性对运算（标志为 p）。相比较前三种运算，散列运算和异或运算的耗时对整体效率的影响可以忽略不计。在本文方案中，签密阶段，n 个签密者在计算 $Q_{i1}=k_iX_B$，$Q_{i2}=t_i(R_B+\ P_{pub}H_1(ID_B,\ R_B,X_B))$ 时，需要用到 $2n+1$ 次点乘运算（$P_{pub}H_1(ID_B,\ R_B,X_B)$ 的值固定，只需计算一次）；在解签密阶段，验证等式计算 $SP=\sum_{i=1}^{n}K_i+\sum_{i=1}^{n}T_i\ \ +\sum_{i=1}^{n}[h_{i3}(R_i+P_{pub}H_1(ID_i,R_i,X_i))]+\sum_{i=1}^{n}h_{i4}X_i$ 和计算 $Q_{i1}=K_ix_B$，$Q_{i2}=T_i(r_B+sH_1(ID_B,R_B,X_B))=\ T_iD_B$，共需要 $5n+1$ 次点乘运算。参考文献[18]所给的实验数据，三种运算所花费的时间代价（以毫秒为单位）分别为 $p\approx 20.01$，$E\approx 11.20$，$s\approx 0.83$。从表 1 中看出，对同样多的消息进行聚合签密，本方案相比于文献[12~15]的方案相比，运算效率提升很多，与运算效率相对较高的方案相比，运算效率提升了近 6 倍。从方案的安全性能来看，只有文献[13]和本方案满足公开验证性。综合考虑方案的运算效率和安全性，本方案优于以上四种方案。

表 1 聚合签密方案运算量和安全性能比较

Table 1 Comparison of computation and security performance of aggregation signcryption

方案	签密	解签密	运算总量	代价估耗	安全性	公开验证性
文献[12]	$np+ne$	$(2n+3)p+(n+1)s$	$ne+(3n+3)p+(n+1)s$	$72.06n+60.86$	可证安全	是
文献[13]	$n(p+2s)$	$(n+3)p$	$(2n+3)p+2ns$	$41.68n+60.03$	可证安全	否
文献[14]	$ne+4ns$	$(n+2)p+ns$	$ne+5ns+(n+2)p$	$35.36n+40.02$	可证安全	否
文献[15]	$3ne+np+ns$	$np+ns$	$2np+3ne+2ns$	$75.28n$	可证安全	否
本方案	$(2n+1)s$	$(5n+1)s$	$(7n+2)s$	$5.81n+1.66$	可证安全	是

4 结束语

聚合签密因其加密、签名和批量处理的特性在物联网环境中具有很大的应用价值。为了提高无证书聚合签密的计算效率，在随机预言模型的基础上，提出了无双线性对的聚合签密方案，经证明该方案满足机密性、不可伪造性和可公开验证性。与已有的方案相比，本方案的计算速度更快，更适合在物联网中应用。

参考文献：

[1] Presser M, Barnaghi P, Eurich M, *et al.* The sensei project: integrating the physical world with the digital world of the network of the future [J]. IEEE Communications Magazine, 2009, 47 (4): 1-4.

[2] Han Jinsoo, Park W K, Lee I, *et al.* Home-to-home communications for smart community with Internet of things [C]// Proc of Consumer Communications& NetworkinG Conference. Piscataway, NJ: IEEE Press,



2017: 720-723.

[3] Lanotte R, Merro M. A semantic theory of the Internet of things [C]// Proc of International Conference on Coordination Languages and Models. Berlin: Springer, 2016: 157-174.

[4] Palade A, Cabrera C, Li Fan, *et al*. Middleware for Internet of things: an evaluation in a small-scale IoT environment [J]. Journal of Reliable Intelligent Environments, 2018, 1 (4): 1-21.

[5] Baldini G, Skarmeta A, Fourneret E, *et al*. Security certification and labelling in internet of things [C]// Proc of the 3rd IEEE World Forum on Internet of Things. Piscataway, NJ: IEEE Press, 2016: 627-632.

[6] Zheng Yuliang. Digital signcryption or how to achieve cost (signature & encryption) ≪cost (signature) +cost (encryption) [C]// Proc of International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 1997: 165-179.

[7] Baek J, Steinfeld R, Zheng Yuliang. Formal proofs for the security of signcryption [J]. Journal of Cryptology, 2007, 20 (2): 203-235.

[8] Selvi D S, Vivek S S, Shriram J, *et al*. Identity based aggregate signcryption schemes [C]// International Conference on Progress in Cryptology-indocrypt. Berlin: Springer, 2009: 378-397.

[9] 张玉磊，李臣意，王彩芬，等. 无证书聚合签名方案的安全性分析和改进 [J]. 电子与信息学报，2015, 37 (8): 1994-1999. (Zhang Yulei, Li Chenyi, Wang Caifen, *et al*. Security analysis and improvements of certificateless aggregate signature schemes [J]. Journal of Electronics & Information Technology, 2015, 37 (8): 1994-1999.)

[10] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [J]. Asiacrypt, 2003, 2894 (2): 452-473.

[11] Barbosa M, Farshim P. Certificateless signcryption [C]// Proc of ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2008: 369-372.

[12] Eslami Z, Pakniat N. Certificateless aggregate signcryption: security model and a concrete construction secure in the random oracle model [J]. Journal of King Saud University-Computer and Information Sciences, 2014, 26 (3): 276-286.

[13] 刘建华，赵长啸，毛可飞. 高效的无证书聚合签密方案 [J]. 计算机工程与应用，2016, 52 (12): 131-135. (Liu Jianhua, Zhao Changxiao, Mao Kefei. Efficient certificateless aggregate signcryption scheme based on XOR [J]. Computer Engineering and Applications, 2016, 52 (12): 131-135.)

[14] 牛淑芬，牛灵，王彩芬，等. 一种可证安全的异构聚合签密方案 [J]. 电子与信息学报，2017, 39 (5): 1213-1218. (Niu Sufen, Niu Ling, Wang Caifen, *et al*. A provable aggregate signcryption for heterogeneous systems [J]. Journal of Electronics & Information Technology, 2017, 39 (5): 1213-1218.)

[15] Han Yiliang, Chen Fei. The multilinear maps based certificateless aggregate signcryption scheme [C]// Proc of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Piscataway, NJ: IEEE Press, 2015: 92-99.)

[16] Lin Jie, Yu Wei, Zhang Nan, *et al*. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications [J]. IEEE Internet of Things Journal, 2017, 4 (5): 1125-1142

[17] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures [J]. Journal of Cryptology, 2000, 13 (3): 361-396.

[18] Deng Lunzhi, Zeng Jiwen, Qu Yunyun. Certificateless proxy signature from rsa [J]. Mathematical Problems in Engineering, 2014, 2014 (9): 1-10.